

“The Damage from Data Disaster”

Whether you are a Corporation with millions of dollars in revenues relying on a Wide Area Network and departmentalized Local Area Networks or a small business using a LAN with a few workstations, your business or organization may be one of the 82% of enterprises that actually lack effective protection against data loss and downtime. This alarming percentage was published in a recent Vulnerability Index Study.

Data disaster, as distinguished from the minor annoyances of workstation malfunctions, involves the massive loss of data or the prolonged interruption of access to data caused by network failure. Causes for the data loss might include the rapid spread of a data destroying virus, damage to equipment from electrical storms, or extensive fire damage to your facility. Your vulnerability is measured by three factors:

1. How dependent are your operations on the storage and retrieval of computerized data?
2. What preventative measures do you have in place?
3. In the event of a serious problem what are your emergency plans for recovery?

Vulnerability Measured in Dollars

To evaluate the need for preventative measures and emergency recovery plans, as well as to justify and quantify the amount of the investment in prevention and the preparation for recovery, you must first assess the potential cost of data disaster.

To make this evaluation, answer the following questions:

- What would be the cost in downtime from an interruption of access to your data?
 - From lost sales?
 - From interrupted productivity or the delivery of services?
 - From the impact on customer or client relations?
- What would be the cost of recreating the lost data?
 - In labor?
 - In necessary equipment?
 - In outside support?
- Is there a potential legal liability associated with the loss of data or the inability to satisfy the conditions of contracts?

Protection Provided by Prevention

Without adequate measures for prevention, recovery will become more difficult and costly.

Adequate Back Up and Storage of Recovery Disks and Equipment Information.

Do you have adequate back-up systems in operation network wide? The issue of back up is a topic in itself and is the cornerstone of prevention.

How frequently do you perform back-ups? Of your servers? Of workstations, if data is stored on them? How frequently is enough? Weekly, daily, more frequently? The answers to that question are other questions: how long would it take to recreate the data during the period that has not been backed-up, and what would it cost to do so? Any interval during which data is not backed up is too long if the cost of recreating the data is unacceptable.

Most systems for adequate back-ups involve storage of a current set of back up media off-site, for the obvious reason that tapes or other storage media could be destroyed in the event of a physical disaster in the primary location.

Are the back-up systems routinely tested? This aspect of a back-up system is the most frequently neglected in smaller companies and organizations.

Is all of your equipment thoroughly documented including

- Serial numbers
- Passwords
- e-mail addresses
- Nomenclatures

Will documentation, installation disks, and start-up disks be readily available? Are these replicated off-site?

Uninterruptible Power Supplies (UPS's)

UPS's help prevent the loss of data in RAM and the corruption of files when an interruption in the power supply occurs while a file is in memory or is being read or written to a disk. They can keep a server running and buy time for a controlled shutdown.

Redundancy

Redundancy involves the duplication of any critical component of your information system including:

- Off site storage of back ups
- Replacement hardware
- Disk duplication systems like mirroring, duplexing, and RAID, which permit a seamless shift from one hard drive to another identical drive in the event of drive failure.

Worst Case Scenario: Emergency Recovery

The best preventative measures cannot in fact always prevent a disaster. They can, however, make recovering from one much easier and less costly. To further reduce your vulnerability to data disaster, you should have an emergency recovery plan.

Some of the questions you will need to answer are:

1. Who will constitute the emergency recovery team?
2. Could some of the recovery procedures be performed off-site in the event of a physical disaster?
3. What are the priorities of operations to be restored in order to minimize costs of downtime?
4. Are external resources required and, if so, should the formulation of the emergency plan be coordinated with these outside sources?

These are a few of the questions that will have to be answered before you can develop a step-by-step emergency disaster plan.

If you are one of the 82% of businesses and organizations who are vulnerable to a data disaster, you have probably rationalized, “The odds are excellent that a true disaster will not happen to me.” Consider the alternatives. What would be the cost if it did? Is the risk worth it? The precautions and planning involved in prevention and developing a recovery plan, can also reduce the cost of relatively minor interruptions of data flow, and may ultimately be worthwhile for that benefit alone.

McGill, Power, Bell & Associates, LLP can assist you to analyze your management information needs and consult with you on the development of a system to meet those needs. But the best systems design is incomplete if it does not include provisions for protecting against and recovering rapidly from an interruption of the flow of that critical management information.

---John E. Litzinger, CPA

Editor's Note --- John is a Partner in the firm's Meadville Office and manages many of the firm's

*Information Technology operations.
He Chairs the Information Technology
Committee and supervises services
such as data processing and payroll
processing; information technology
consultation; and installation and
support for various software solutions.*